

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/28/2010 has been entered.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Kenneth Fields on 1/13/2012.

Please amend the application as follows:

Claims 14, 25, and 42 should be amended to the claim language as shown below. These amended claims will **replace** claims 14, 25, and 42 as filed on 7/28/2010:

In claim 14, the amendment filed on 7/28/2010 **has been changed to** -- A terminal apparatus to which a piece of unique information being a base of a decryption key for decrypting

a piece of encrypted data is assigned by a management apparatus that manages, with use of a tree structure, a plurality of apparatus identifiers identifying a plurality of terminal apparatuses,

~~wherein the management apparatus (i) calculates and generates, for each of nodes in layers except for leaves of the tree structure, a subset defined, by a subset difference, as a set being made up of one or more apparatus identifiers positioned subordinate to the node, (ii) searches, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and performs a first association for associating the another subset as an association source with the subset as an association destination, (iii) searches for another subset that wholly contains the containing subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and performs a second association for associating the subset as a new association source with the another subset as a new association destination, (iv) controls a second association unit so that the associating is repeatedly performed up to an uppermost layer, (v) performs control so that the first association, the second association, and the control on the second association unit are repeatedly performed on all subsets generated for respective nodes in the lowermost layer, (vi) performs a first assignment for bringing pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in lowermost layer, and (vii) performs a second assignment for~~

bringing, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information, and

the terminal apparatus includes comprising:

a unique information storing unit storing therein a piece of unique information that contains an apparatus identifier of the terminal apparatus, out of the pieces of unique information that have been distributed from the management apparatus in advance and are brought into correspondence with the a plurality of subsets,

wherein the management apparatus (i) calculates and generates, for each of nodes in layers except for leaves of the tree structure, a subset defined, by a subset difference, as a set being made up of one or more apparatus identifiers positioned subordinate to the node, (ii) searches, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated for a parent node of the node positioned in an immediately upper layer thereof, and performs a first association for associating the another subset as an association source with the subset as an

association destination, (iii) searches for another subset that wholly contains the containing subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated for a parent node of the node, and performs a second association for associating the subset as a new association source with the another subset as a new association destination, (iv) controls a second association unit so that the associating is repeatedly performed up to an uppermost layer, (v) performs control so that the first association, the second association, and the control on the second association unit are repeatedly performed on all subsets generated for respective nodes in the lowermost layer, (vi) performs a first assignment for bringing pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in lowermost layer, and (vii) performs a second assignment for bringing, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information.--

In claim 25, the amendment filed on 7/28/2010 **has been changed to** --A copyright protection system comprising:

a plurality of terminal apparatuses; and

a management apparatus that manages the plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to be bases of decryption keys for decrypting a piece of encrypted data to the apparatus identifiers respectively, ~~wherein~~

wherein the management apparatus includes:

a subset generating unit operable to calculate and generate, for each of nodes in layers except for the leaves of the tree structure, a subset defined, by a subset difference, as a set being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association unit operable to search, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and to associate the another subset as an association source with the subset as an association destination;

a second association unit operable to search for another subset that wholly contains the subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and

to associate the subset as a new association source with the another subset as a new association destination;

a first control unit operable to control the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control unit operable to control the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets generated for respective nodes in the lowermost layer;

a first assignment unit operable to bring pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer, and to assign each piece of unique information to apparatus identifiers contained in the respective subset in the lowermost layer; and

a second assignment unit operable to bring, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and the pieces of new unique information derivatively obtained from the pieces of unique information.--

In claim 42, the amendment filed on 7/28/2010 has been changed to --A non-transitory computer-readable program recording medium which records thereon a program that is for making associations and has a management apparatus execute the following steps, the management apparatus managing a plurality of a plurality of terminal apparatuses by arranging apparatus identifiers for identifying the plurality of terminal apparatuses to be leaves of a tree structure and assigning pieces of unique information to the apparatus identifiers, the pieces of unique information being bases of decryption keys for decrypting a piece of encrypted data, the steps being:

a subset generating step of calculating and generating, for each of nodes in layers except for the leaves of the tree structure, a subset defined, by a subset difference, as a set being made up of one or more apparatus identifiers positioned subordinate to the node;

a first association step of searching, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and associating the another subset as an association source with the subset as an association destination;

a second association step of searching for another subset that wholly contains the subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and to associate the subset as a new association source with the another subset as a new association destination;

a first control step of controlling the second association unit so that processing thereof is repeatedly performed up to an uppermost layer;

a second control step of controlling the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets generated for respective nodes in the lowermost layer;

a first assignment step of bringing pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer and assigning each piece of unique information apparatus identifiers contained in the corresponding subset in the lowermost layer; and

a second assignment step of bringing for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with one or more subsets being association destinations and assigning each piece of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information.--

Allowable Subject Matter

Claims 1-36, 39, 40, and 42 are allowed.

The following is an examiner's statement of reasons for allowance: The above mentioned claims are allowable over the prior arts because the CPA (Cited Prior Arts) of record taken singly or in combination fail to anticipate or render obvious the specific added limitations, as recited in independent claims 1, 14, 25, 39, 40, & 42 and subsequent dependent claims.

Applicant's amendments and pages 2-5 of the remarks filed 7/28/2010 overcome the cited prior arts of records.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Kim can be reached at (571) 272-3804. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
1/13/2012

NK

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2494